WE CLAIM:

1. A method for establishing a secure connection between a client platform and a service, comprising:

downloading a digitally signed applet from the service to the client platform;

verifying the digitally signed applet at the client platform using a first public key the client platform already knows and trusts;

executing the applet at the client platform, thereby controlling the client platform to store a second public key corresponding to the server; and

using the stored second public key to authenticate the service and establish the secure connection.

2. The method of claim 1 wherein the applet includes first program code that controls the client platform to store the second public key to a non-volatile memory.

3. The method of claim 2 wherein the non-volatile memory comprises disk.

4. The method of claim 2 wherein the applet further includes second program code that controls the client platform to use the stored second public key to verify a signature subsequently provided by the server.

5. The method of claim 1 wherein the applet further includes program code that controls the client platform to use the stored second public key to verify a signature subsequently provided by the server.

6. The method of claim 1 wherein the executing step includes controlling the client platform to store a second public key in the form of a digital certificate corresponding to the server, and the using step comprises receiving a digital signature from the server, and authenticating the received digital signature under control of the executing applet through use of the stored digital certificate corresponding to the server.

7. The method of claim 1 wherein the using step includes having the executing applet invoke a further applet to establish a secure connection.

8. The method of claim 1 wherein the applet comprises a signed Java Archive containing a digital certificate corresponding to the server, and a program fragment that stores the digital certificate in a predetermined location on the client platform that permits the client platform to later retrieve the stored digital certificate.

9. A client platform for establishing a secure connection with a service over a network, comprising:

an applet receiver that receives a digitally signed applet from the service over the network;

an applet verifier that verifies the digitally signed applet using a first public key the client platform already knows and trusts;

an applet executor that executes the applet, thereby controlling the client platform to store a second public key corresponding to the server, and uses the stored second public key to authenticate the service and establish the secure connection.

10. A method for establishing a secure connection with a client, comprising:

downloading an applet to the client platform, the digitally signed applet being digitally signed such that the client platform can verify the digitally signed applet using a first public key the client platform already knows and trusts, the digitally signed applet including a second public key and code that controls the applet to store the second public key on the client platform;

sending a digital credential to the client, said digital credential being verifiable by the client platform using the stored second public key; and establishing a secure communication with the client based on said digital credential as verified by the client.

11. The method of claim 10 wherein the applet code controls the client platform to store the second public key to a non-volatile memory.

12. The method of claim 11 wherein the non-volatile memory comprises disk.

13. The method of claim 10 wherein the applet further includes further code that controls the client platform to use the stored second public key to verify the digital credential.

14. The method of claim 10 further including sending a further applet to the client platform in response to an invocation of the further applet by the first-mentioned applet.

15. The method of claim 10 wherein the applet comprises a signed Java Archive containing a digital certificate, and a program fragment that stores the digital certificate in a predetermined location on the client platform that permits the client platform to later retrieve the stored digital certificate.

16. A server for establishing a secure connection with a client over a network, comprising:

an applet transmitter that transmits a digitally signed applet to the client over the network, the applet being digitally signed using a first public key the client already knows and trusts, the applet including a program that controls the client to store a second public key corresponding to the server; and

a digital credential transmitter that transmits a digital credential to the client executing the applet, the digital credential being authenticatable by the second public key.

17. A method for establishing a secure connection between a server and a web browser having access to a first, trusted public key, comprising:

downloading a digitally signed item from the server to the browser, the item including a second public key;

verifying the digitally signed item at the browser using the first public key;

storing the second public key in response to the verifying step; and

using the stored second public key to authenticate the server.

18. A method as in claim 17 wherein the item comprises a Java archive.